

CLAIMS

What is claimed is:

1. A method for authenticating transferred data between a sender and a receiver over an open network comprising the steps of:

5 establishing a first secure transmission of data between the sender and the receiver;

transmitting at least one token to the receiver during the first secure transmission;

10 establishing at least one additional transmission of data between the sender and the receiver;

transmitting the data and at least one token during the at least one additional transmission; and

15 comparing the at least one token transmitted during the at least one additional transmission to the at least one token transmitted during the first secure transmission to determine whether the transmission is authentic.

2. The method according to claim 1, wherein the at least one token comprises a preselected number of tokens.

3. The method according to claim 2, wherein the number of at least one transmissions corresponds to the preselected number of tokens.

4. The method according to claim 2, wherein the number of at least one transmissions is greater than the preselected number of tokens.

5. The method according to claim 2, wherein the number of at least one transmissions is less than the preselected number of tokens.

6. The method according to claim 1, wherein the at least one additional transmission is conducted over an unsecure or open connection.

7. The method according to claim 1, wherein the first secure transmission is encrypted.

8. The method according to claim 1, wherein the at least one additional transmission is sent in plaintext.

9. The method according to claim 5, wherein the at least one additional transmission is sent in plaintext.

10. The method according to claim 2, wherein the first secure transmission is encrypted.

11. The method according to claim 3, wherein the at least one additional transmission is sent in plaintext.

12. The method according to claim 1, further comprising the steps of transmitting a checksum value during the first transmission and having the receiver verify that the checksum value is accurate by comparing the transmitted value to a checksum value generated using a similar checksum algorithm.

13. The method according to claim 10, wherein the transmitted checksum value is based upon checksum values transmitted during previous transmissions.

14. A method for securely transferring data between a sender and a receiver over an open network comprising the steps of:

establishing a first secure transmission between the client and the server which is encrypted;

transmitting a preselected number of tokens to the server during the first secure transmission;

establishing a number of additional transmissions between the client and the server corresponding to the preselected number of tokens;

transmitting the data and one of the preselected tokens during each additional

transmission;

comparing the transmitted token during the additional transmission to the corresponding token transmitted during the first secure transmission.

5 15. The method according to claim 14, wherein the additional transmissions are sent in plaintext.

 16. The method according to claim 14, further comprising the steps of transmitting a checksum value during the first transmission and having the receiver verify that the checksum value is accurate by comparing the transmitted checksum value to a checksum value generated using a similar algorithm.

10 17. The method according to claim 16, wherein the transmitted checksum value is based upon checksum values transmitted during previous transmissions during this transaction.

 18. The method according to claim 1, wherein the number of additional transmissions is variable and adaptively selected.

15 19. The method according to claim 18, wherein the number of additional transmission is adaptively selected, at least in part, based upon the performance overhead of the system.

20. The method according to claim 18, wherein the number of additional transmissions is adaptively selected, at least in part, based upon monitored conditions.

21. The method according to claim 18, wherein the number of additional transmissions is adaptively selected, at least in part, based upon a set of criteria that are used in an algorithm to determine the number of additional transmissions, the criteria selected from the group consisting of the frequency of transmissions between the sender and receiver, the closeness of the sender to the source of the transactions, and the usage patterns of the client.

22. The method according to claim 22, wherein the algorithm is a statistical averaging algorithm.

add
as